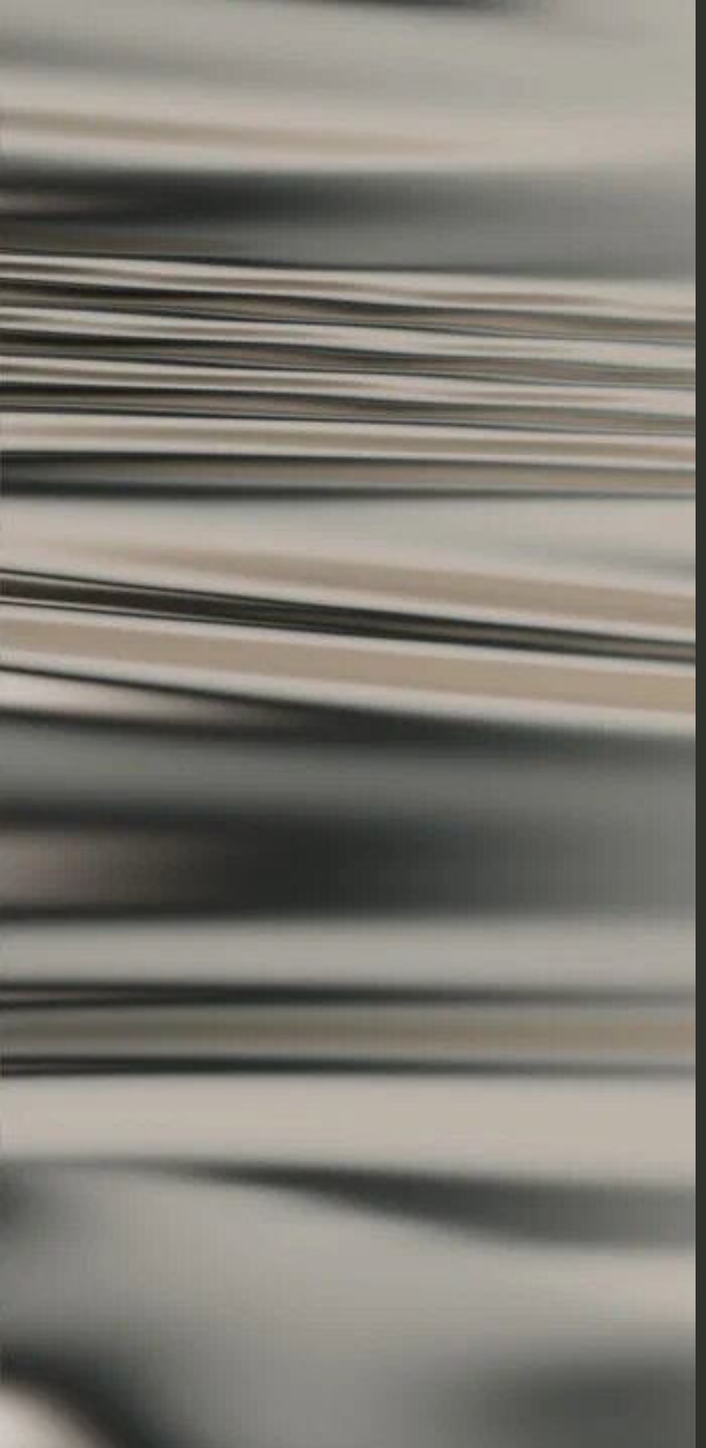
BFS OmniVideo

Banking Financial Systems

Омниканальное видеорешение
для удаленного обслуживания Клиентов

BFS™



БФС OmniVideo – это система, которая помогает банкам решать задачу очной консультации и идентификации при помощи дистанционного подключения оператора в доступном для пользователя канале и дает возможность увеличить зоны присутствия без необходимости строительства новых офисов

Работа в режиме 24/7/365
обслуживание клиентов в удаленных каналах

Быстрое расширение точек присутствия Банка
устройство легко установить в любом, даже удаленном, регионе

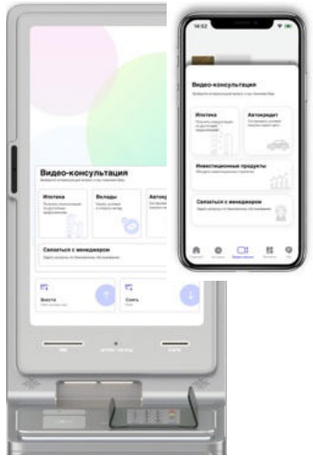
Мини-офис
пользователи могут провести более 95% операций, доступных в офисе Банка

Современный и удобный способ взаимодействия с Банком
человек может связаться с квалифицированным сотрудником Банка в любое время

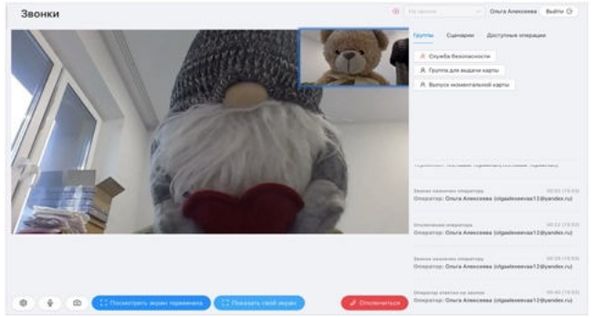
Безопасность
решение полностью устанавливается во внутреннюю сеть Банка

Функциональные блоки системы

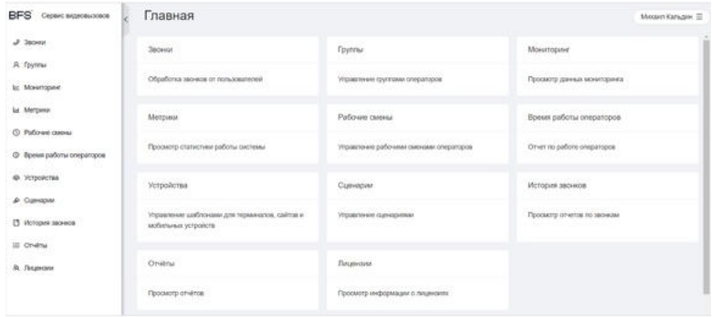
Каналы



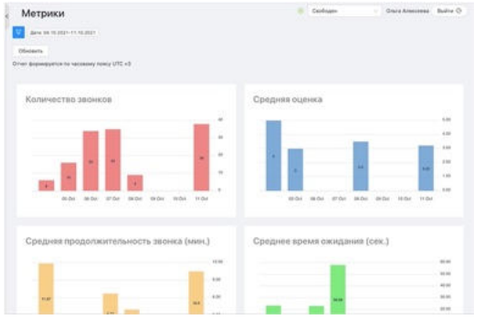
Инструменты для обслуживания клиента



Панель администрирования

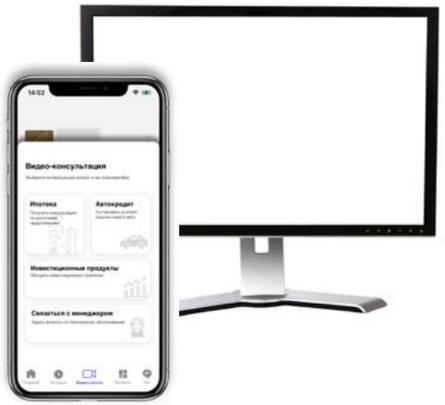


Аналитические инструменты



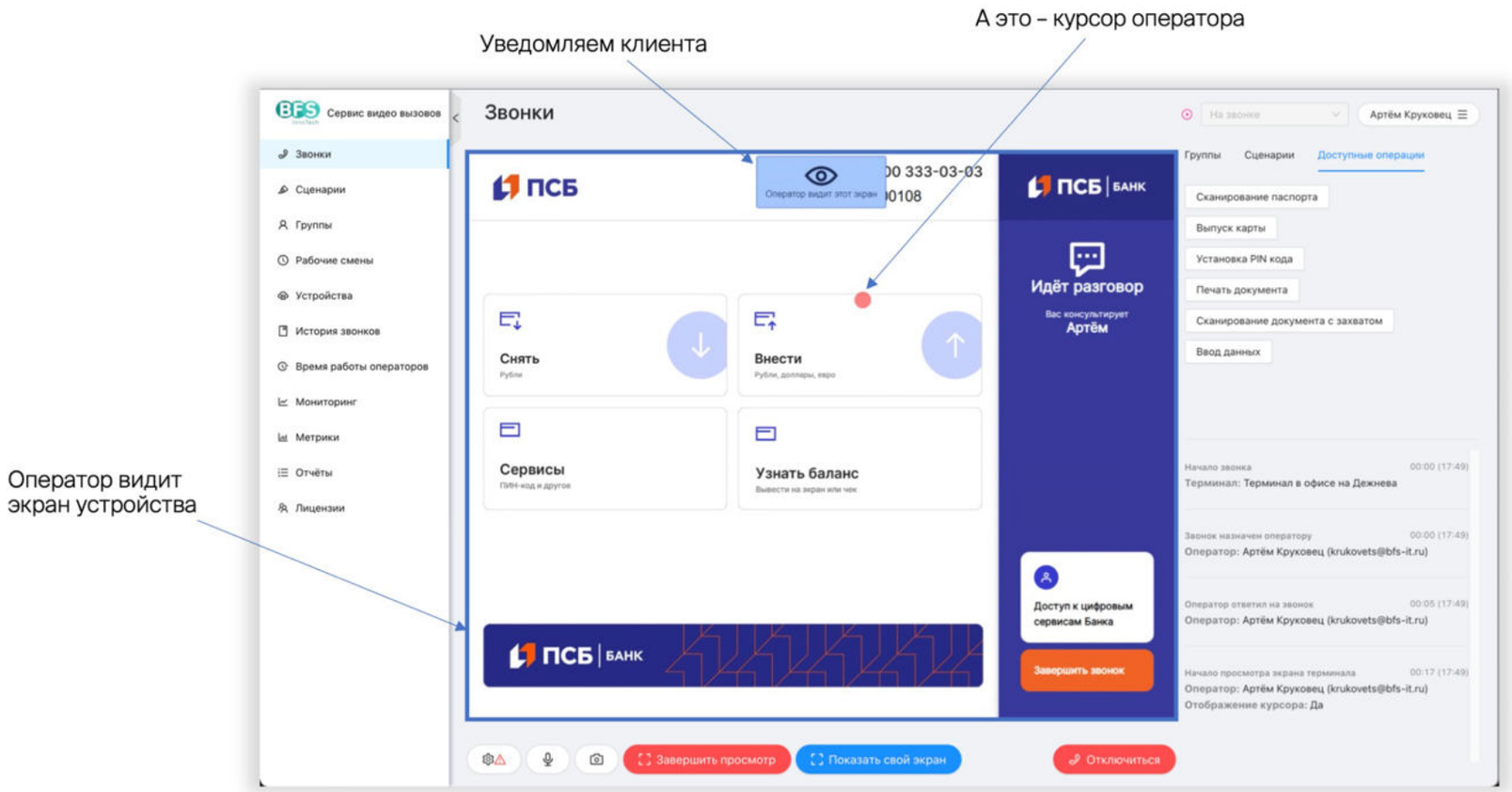
Каналы и возможности

- Видео консультация
- Отправка файлов и печать документов
- Планшетный сканер для документов
- Сканирование паспорта в разных спектрах
- Сканер протяжный с захватом документа
- Дистанционная выдача физической карты
- Активация продукта



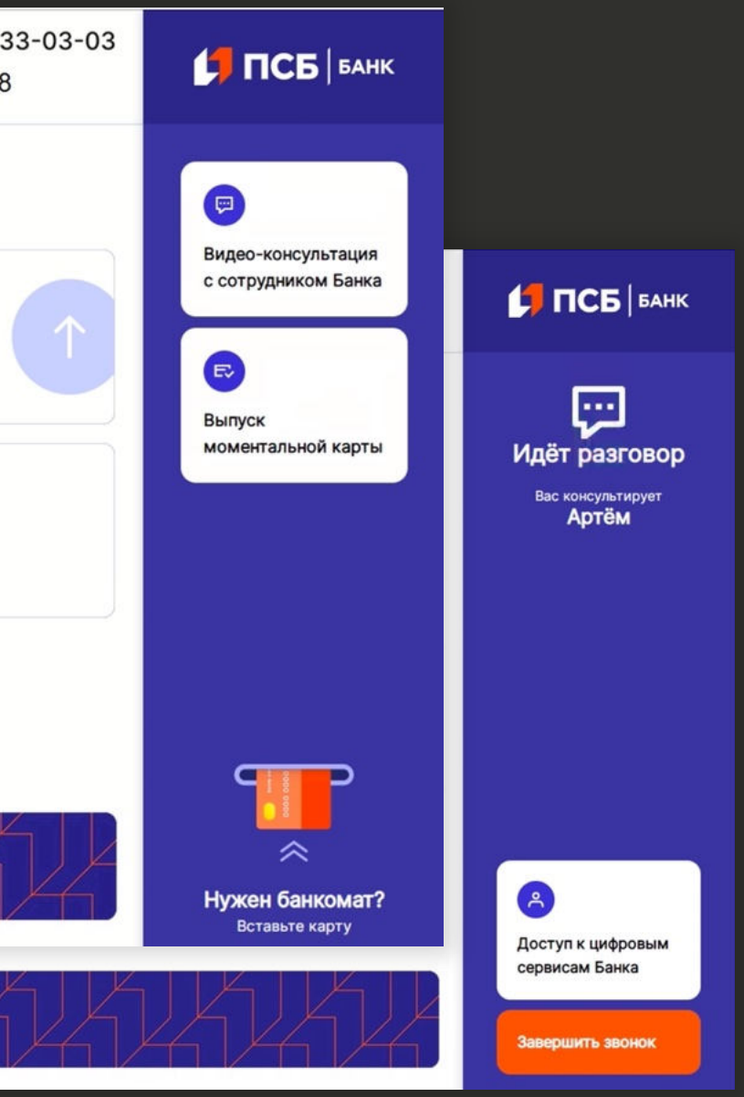
- Видео консультация
- Отправка файлов

Интерфейс оператора



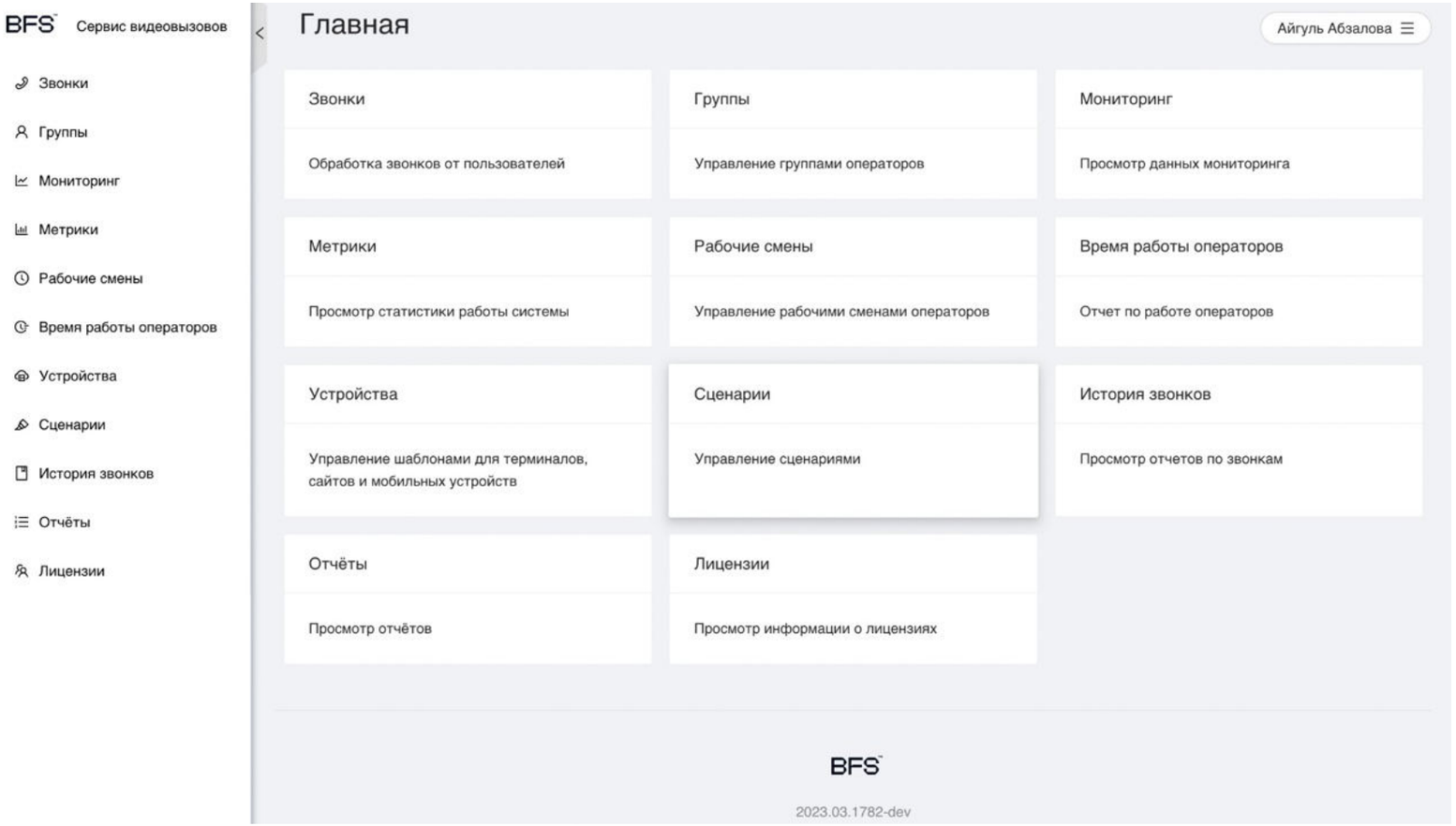
- Управление статусом оператора
- Выбор сценария бизнес-процесса
- Co-browsing
- Передача звонка между операторами и группами
- Выполнение операций на терминале (например, выдача карты)

Процесс обслуживания



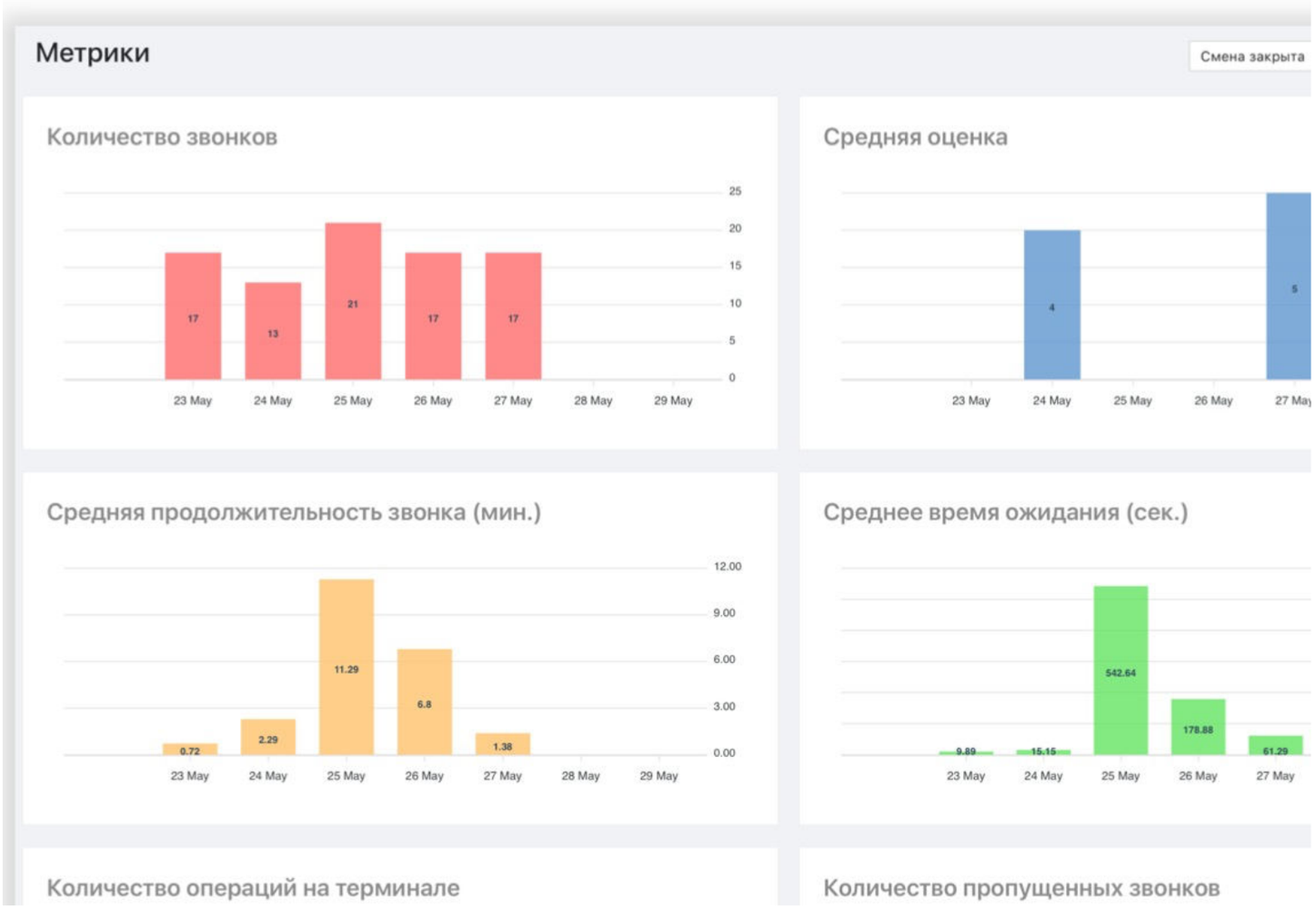
1. Потенциальный клиент в интерфейсе устройства выбирает пункт «Видео-консультация»
2. Программное решение соединяет потенциального клиента со свободным сотрудником видео колл-цента Банка, начинает запись видеосеанса.
3. В режиме видеосеанса сотрудник Банка проводит удаленную идентификацию путём сканирования паспорта потенциального клиента через сертифицированный сканер паспорта, установленный в устройстве.
4. После проверки документа, оператор предоставляет доступные для потенциального клиента банковские услуги.
5. При необходимости подписания документов, оператор печатает их на устройстве и через специализированный модуль со сканером принимает их во внутреннее хранилище.
6. В случае, если пользователь уже является клиентом Банка, оператор предоставляет ему возможность управлять своими банковскими продуктами, в том числе, открывать новые, например, достоверно заключить кредитный договор.

Панель администрирования



- Управление ролями и группами
- Управление доступами
- Управление сценариями с использованием периферии
- Маршрутизация звонков
- Управление набором услуг на терминалах
- Настройка клиентского меню

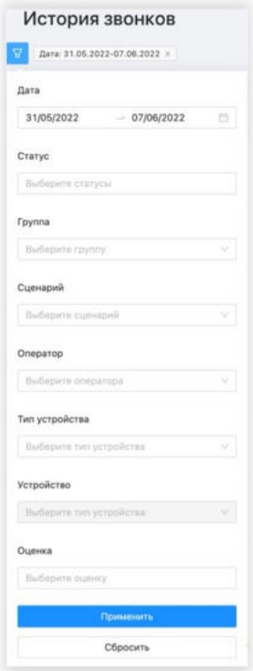
Аналитические инструменты – метрики

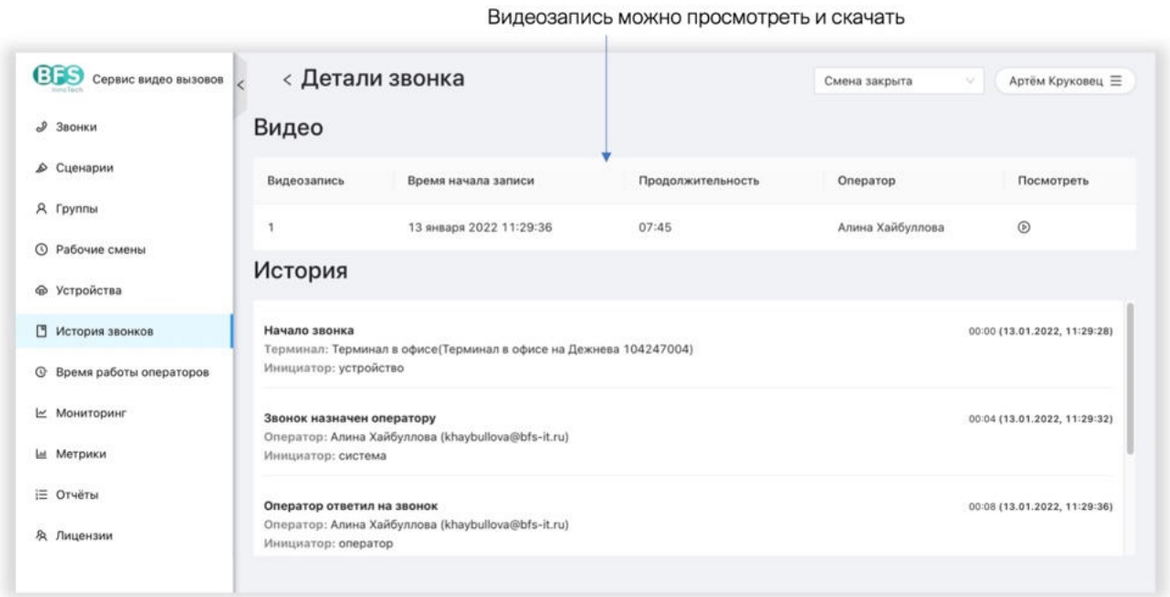


Отслеживание метрик:

- Количество звонков
- Средняя оценка качества
- Продолжительность звонка
- Среднее время ожидания
- Количество операций на терминале
- Количество пропущенных звонков
- Фильтрация по устройству, оператору, периоду

Аналитические инструменты - история звонков





Просмотр истории звонков:

- Полная история
- Фиксация всех событий
- Просмотр документов
- Выгрузка документов
- Просмотр записи видеосеанса
- Выгрузка записи видеосеанса

Основные технические характеристики

- Поддержка видеосвязи в режиме реального времени с разрешением до 1080p (FullHD)
- Встроенные алгоритмы адаптации качества видео в зависимости от качества канала связи
- Поддержка TLS 1.2+, сквозного шифрования
- Запись видеосеансов и истории обслуживания
- Серверные компоненты работают на отечественных Linux-дистрибутивах
- Решение полностью разработано в России
- Решение входит в реестр Минцифры РФ
- Поддержка работы с аппаратно-программными комплексами ГОСТ-шифрования
- Сканер паспорта имеет необходимые сертификаты для работы с российскими документами

Известные риски и их минимизация

Риск при видеоидентификации	Механизмы снижения риска
Оспаривание процедуры идентификации	Фиксация процедуры идентификации. Получение собственноручных подписей.
Подлог данных	Проверка предоставленных документов и информации по независимым первичным источникам информации.
Использование украденных документов	Двухфакторная аутентификация – процедуры, которые в соответствующем контексте позволяют определить принадлежность документа или данных клиенту.
Деятельность в интересах третьих лиц	Мониторинг транзакций на предмет выявления паттернов, не соответствующих профилю клиентов или указывающих на высокий риск незаконной деятельности.
Использование синтетических подтверждений личности	Проверка предоставленных документов и информации по независимым первичным источникам информации. Информация проверяется в совокупности.
Кибер-риски	Использование защищенных каналов связи. Мониторинг подозрительной активности. Внешние аудиты информационных систем.
Внутреннее мошенничество	Внутренний мониторинг. Скрининг сотрудников. Правило «четырех глаз». Видеофиксация процедуры идентификации клиента.
Действие по принуждению	Использование видеоконтроля, соответствующее размещение банкоматов, использование «красной кнопки».
Взаимодействие с инсайдерами, коррупция	Исключение физического контакта с оператором, выбор случайного оператора.
Использование поддельного изображения, deepfakes	Исключение возможности доступа к оборудованию и каналам связи со стороны пользователя.

BFS™

+7 (495) 223-06-27
www.bfs.su
www.bfs-it.ru